Foto: wordpress.com

Ciberguerra,

la nueva amenaza mundial del siglo XXI. Colombia y el reto de la cultura de información.

Coronel (RA)
Jairo Andrés Cáceres García
Docente investigador de la cátedra de Ciberguerra en la ESDEGUE.

La información es hoy el principal activo de las organizaciones, tanto en el sector público como en el privado. En ese marco, la Defensa se constituye en el primer eslabón de la cadena de blindaje preventivo contra la ciberguerra, el cibercrimen y sus diferentes modalidades. Este artículo pretende llamar la atención del lector sobre la necesidad imperiosa de tener una buena cultura de Seguridad de la Información, para minimizar el riesgo de incidentes de seguridad. Así mismo, como lo dice el título, la seguridad de la información es la clave del éxito en el proceso de minimizar el riesgo en caso de un ciberataque o una ciberguerra.

La Escuela Superior de Guerra desde 2011 asumió un proceso de investigación por intermedio del Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales, CEESEDEN, en la línea de Investigación, Desarrollo Científico, Tecnológico e Innovación, con el objetivo de ahondar en el tema de la tecnología, en especial, en lo referente a las tecnologías de punta y sus nuevas amenazas.

El desarrollo de la tecnología ha sido tan rápido y significativo que está presente en todos los sectores de la sociedad. Todo su andamiaje tecnológico requiere, en consecuencia, control y orden. En el siglo XXI, vivimos con mayor intensidad la inseguridad de la información, lo que no es solo un problema actual, pues desde tiempos inmemoriales se han presentado incidentes con la información, como en la época de los romanos, «que fueron maestros en imitar y apropiarse en lo más ventajoso de los enemigos…» (Diccionario Militar español, edición 1869). El presente trabajo quiere llamar la atención sobre la necesidad imperiosa de tener una cultura de Seguridad de la Información, para minimizar el riesgo de incidentes. En especial, de tomar medidas preventivas o defensivas en caso de presentarse un ciberataque o, peor aún, una ciberguerra.

Este tema es de vital importancia, tanto que está contemplado en las *nuevas amenazas* del siglo XXI. Así mismo, los activos de la información, que son todo aquello que tiene valor para las organizaciones, como por ejemplo, hojas de vida, historias clínicas, bases de datos, archivos de datos, contratos, acuerdos, facturas, planes, estrategias de negocios e información confidencial de Seguridad y Defensa Nacional, entre otros, están permanentemente en riesgo por amenazas internas o externas. Además de ser requeridos por todas las instituciones, el conocimiento de las bases de datos personales, con un mayor riesgo de afectar la intimidad.

La información es hoy el principal activo de las organizaciones, tanto en el sector público como en el privado. En ese marco, la Defensa se constituye en el primer eslabón de la cadena de blindaje preventivo contra la ciberguerra, el cibercrimen y sus diferentes modalidades.

El asunto cobra más importancia si se tiene en cuenta que cada día los países, las empresas y los gobiernos son más dependientes de la tecnología, lo que pone en un alto riesgo de incidente de seguridad o ataque cibernético a su infraestructura crítica, bien sea en la reserva de un avión o en los servicios públicos, por ejemplo.

Foto: Norwegian Information Security laboratory Department of Computer Science and Media Technology

El 80 % de la infraestructura crítica de los Estados Unidos está en manos del sector privado, soportado sobre sistemas de información, lo que los hace muy vulnerables y de difícil defensa de ciberataques, motivo por el cual el presidente Obama, ha ordenado la creación de un sistema de donación voluntario para ayudar a proteger a las empresas que tienen bajo su responsabilidad la infraestructura crítica que podrían ser amenazadas como las dedicadas a la distribución de agua y energía.

1. ¿Qué se entiende por Seguridad de la Información?

Es un proceso que busca proteger la información, contra un compendio de amenazas, en pro de asegurar la continuidad del negocio, disminuir los posibles daños y maximizar el retorno de la inversión de la organización.

Así mismo, se puede definir como la garantía del servicio enfocado desde tres puntos de vista:

- el funcionamiento correcto de la infraestructura tecnológica instalada
- la integridad de la información, datos y programas, tanto en su soporte como en el adecuado empleo
- el mantenimiento a un buen nivel de calidad y fiabilidad de la información suministrada, tanto en contenido como en oportunidad

La Norma ISO 27001 (norma internacional que certifica en los estándares en Seguridad de la Información y define cómo organizar la seguridad de la información en cualquier tipo de organización, esta norma es para la seguridad de la información lo mismo que ISO 9001 es para la calidad) determina la seguridad de la información como la preservación de varios componentes que en adelante se detallan.

- *Confidencialidad*

  ¿Qué pasa si la información cae en manos de personas no autorizadas, como un delincuente, un reportero o un competidor?

- *Integridad*

  ¿Qué sucede si la información se corrompe, se pierde o se altera accidental o intencionalmente?

- *Disponibilidad*

  ¿Qué pasa si la información no está accesible por cierto tiempo o no está el día y a la hora requerida (ejemplo: la nómina de las FF.MM., clientes de un banco)?

  ¿Cuánto tiempo puede el negocio tolerar esta falta de disponibilidad antes de que empiece a tener impacto o entrar en crisis?

  ¿En qué fecha u horarios es más crítica una falla de disponibilidad?

La Norma ISO27001 es la base para la gestión de la *seguridad de la información*. Es una norma redactada por expertos del mundo en el campo de la seguridad de la información, cuyo objetivo es determinar una metodología para la implementación de la seguridad de la información en cualquier organización.

Muchos países han tomado esta norma como base para determinar las diferentes normas en el área de la protección de datos personales, de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras así como en la Seguridad y Defensa Nacional.

En los últimos años se ha evidenciado una realidad, la alta dependencia tecnológica de las sociedades en especial las desarrolladas, imprescindible para el buen funcionamiento de los Estados, sus Fuerzas Armadas y como ya se citó anteriormente, en los Estados Unidos de Norteamérica, el 80 % de la infraestructura crítica, está en manos del sector privado, lo que constituye un gran riesgo para efectos de la prestación eficiente de los servicios públicos y un alto riesgo para la Seguridad y Defensa Nacional.

«Esta dependencia seguirá aumentando en el futuro. Las tecnologías de la información hacen posible casi todo lo que las Fuerzas Armadas de un país requieren para el cumplimiento de la misión asignada: apoyo logístico, comando y control e información de Inteligencia en tiempo real, entre otros. Todas estas funciones dependen de sus redes de comunicaciones informáticas, que en el caso de EE. UU., por ejemplo, cuentan con más de 15.000 redes y siete millones de terminales informáticos distribuidos en cientos de instalaciones en docenas de países, para cuyo funcionamiento requieren más de 90.000 especialistas.

En menos de una generación, las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico» (Tomado del libro *Cuadernos de estrategia*, 149, del Ministerio de Defensa de España).

2. La cultura de la seguridad de la información

La cultura de seguridad de la información es un conjunto de conocimientos que reconoce en el ser humano su inteligencia emocional, así como sus aciertos y fallas. Con ella se asumen las buenas prácticas de seguridad de la información, como hábitos casi inconscientes, tendientes a minimizar los riesgos de incidentes de seguridad.

Una cultura de seguridad de la información fuerte y consistente no habla de una empresa sin incidentes de seguridad, ni fraudes, sino de una que destruye sus propias autorrestricciones para conocer y atender nuevas formas de vida informática sin equivocarse.

La cultura de la seguridad de la información es un reconocimiento del riesgo, es una percepción del mismo, que mantiene o no alerta a la persona frente a situaciones que pueden vulnerar su espacio individual o comunitario cuando de manejo de información u otra situación se trate. Mientras unos son más proclives a tomar riesgos, otros no tanto.

Una cultura de seguridad de la información no solo requiere especialistas técnicos en tecnologías de seguridad de la información, sino especialistas organizacionales en administración del riesgo, que canalicen los planes de seguridad y control acordes con la percepción y apetito al riesgo de sus participantes.

La cultura de la seguridad de la información es un reconocimiento del riesgo, es una percepción del mismo, que mantiene o no alerta a la persona frente a situaciones que pueden vulnerar su espacio individual o comunitario cuando de manejo de información u otra situación se trate. Mientras unos son más proclives a tomar riesgos, otros no tanto. La exposición a los riesgos depende de nuestras experiencias previas y situaciones que nos han llevado a tomar decisiones para avanzar o ser más prevenidos ante los eventos inesperados.

Cuando nos sentimos más confiados y confortables en nuestro entorno, se percibe una sensación de protección, que nos anima a tomar mayores riesgos y acciones, pues elementos en el contexto de nuestra decisión nos dicen que es posible actuar con tranquilidad y sin miedos. Cuando advertimos un ambiente hostil, poco confiable y lleno de incertidumbre, nuestras acciones podrán ser conservadoras y prudentes, o lanzadas y temerarias, dependerá de nuestro apetito al riesgo y de nuestra historia frente a decisiones similares. Podríamos decir que en entornos agrestes y desconocidos, nuestra memoria de riesgos se activa y percibe los niveles de incertidumbre que podemos manejar y nos cuestiona cuando dichos límites se vulneran o sobrepasan.

Así las cosas, una cultura de seguridad de la información se basa en qué tan bien una organización es capaz de gobernar y administrar los incidentes que se presentan. Cómo se enfrenta la incertidumbre de la falla y sus efectos inesperados. Una cultura de seguridad de la información que encuentra en la inevitabilidad de la falla la fuente de sus supuestos, es capaz de modificar las prácticas expuestas y en uso, en una realidad concreta que se materializa en comportamientos confiables de las personas.

Es decir, una cultura de seguridad que reconoce en los incidentes o materialización de los riesgos, una forma de actuar y conocer qué tan inseguros son, es capaz de construir un lenguaje de seguridad, de percepción, no basado en una visión de invulnerabilidad tecnológica, sino en la confiabilidad de su reacción humana frente a la vulnerabilidad propia de los sistemas. Construir una cultura de seguridad alrededor de los incidentes es destruir la falsa sensación de seguridad y diseñar un sistema preventivo que crea en las buenas prácticas y en el ser humano contingente.

Una cultura de seguridad de la información no solo requiere especialistas técnicos en tecnologías de seguridad de la información, sino especialistas organizacionales en administración del riesgo, que canalicen los planes de seguridad y control acordes con la percepción y apetito al riesgo de sus participantes. No sin antes acotar, que la seguridad supone la exposición a situaciones riesgosas, como una manera de conocer los impactos de las medidas y la efectividad de sus controles.

3. ¿Seguridad de la información o seguridad informática?

Se escucha frecuentemente hablar de seguridad de la información y seguridad informática de modo indistinto. La seguridad informática protege el sistema informático, tratando de asegurar la integridad y privacidad de la información que contiene. Se puede decir que se trata de implantar medidas técnicas que preserven las infraestructuras tecnológicas y de comunicación que soporten la operación de una organización, es decir, los *hardwares* y *softwares* empleados por la organización.

En cambio, la seguridad de la información es un concepto más profundo, ya que intenta implementar medidas de seguridad a otros medios donde se localice información, como impresiones en papel, discos duros e incluso, medidas de seguridad respecto de las personas que la conocen.

Foto: http://blogs.reuters.com/great-debate/files/2013/06/computer-security.jpg

Está orientado no solo a preservar la información, sino además a la mejora de los procesos de negocio, añadiendo a las medidas técnicas, otras organizativas y legales, que permitan a la empresa asegurar con mayor solidez la confidencialidad, integridad y disponibilidad de su sistema de información.

Por lo anterior, se puede afirmar que mientras la seguridad de la información integra toda la información independientemente del medio en que esté (físico o digital), la seguridad informática únicamente atiende a la protección de las instalaciones informáticas y de la información en medios digitales.

La ciberguerra

"Acciones de un Estado-Nación para penetrar en los equipos o redes de otro país, con el fin de causar algún daño o interrupción" (Richard A. Clarke, *Cyber War*)

"Un nuevo dominio en la guerra" (William J. Lynn, U.S., Secretario Adjunto de Defensa).

Estas son dos de las tantas definiciones que hay sobre la ciberguerra en la actualidad, para tener un referente y un contexto sobre el tema que nos ocupa.

Dada la evolución de la tecnología y la dependencia que ha generado su uso especialmente en países desarrollados, (sin desconocer los grandes adelantos y beneficios que le ha traido a la humanidad), diariamente se registra un desmedido auge de delitos informáticos que hacen cada vez más latente la amenaza de una guerra cibernética.

Algunos analistas ya hablan de un *ciber Pearl Habor*, otros de *ciber Hiroshima*, con efectos tan destructivos como una guerra nuclear, que dada la situación actual no se trata de algo que pueda suceder. Ya está sucediendo. Afortunadamente aún no una ciberguerra, pero sí hay frecuentemente ciberataques, que en los periódicos y noticieros están al orden del día.

El Jefe de Defensa Cibernética de la OTAN ha advertido que el terrorismo basado en sistemas informáticos plantea la misma amenaza a la seguridad nacional que un ataque con misiles. Lo dice así: «La Ciberguerra puede convertirse en un problema global muy eficaz porque es bajo el riesgo, bajo el costo, altamente eficaz y fácilmente desplegable a nivel global. Es casi un arma ideal que nadie puede ignorar».

De acuerdo con las declaraciones del Jefe de Defensa Cibernética de ese organismo, puede asegurarse que un inesperado ataque cibernético de mayores consecuencias pone en peligro el orden y la seguridad mundial.

Los ataques contra la infraestructura crítica y los sistemas de información del sector público y privado pueden derivar, en un futuro no muy lejano, en un conflicto militar de gran escala, con consecuencias inimaginables.

Desde esa perspectiva, teniendo claro el preocupante panorama de la ciberguerra y sus incalculables consecuencias en el mundo, se deben tomar medidas para minimizar este riesgo. *La seguridad de la información es el primer eslabón de la cadena que permite reducir o minimizar el riesgo,* pues no existe la garantía total de inmunidad a un ataque *cibernético.* Ningún sistema de información está a salvo de sufrir un ataque de graves consecuencias como robo, pérdida, destrucción, fuga de información, redirección de información para usos fraudulentos, interceptación en proceso, correo no deseado.

Muchos países están desarrollando estrategias nacionales en ciberdefensa con las que persiguen conseguir un ciberespacio más seguro mediante el intercambio de información, alertas tempranas, vulnerabilidades, amenazas, la mejora de su sistema de Contrainteligencia y la mejora de sus productos y tecnologías, así como la concientización de ciudadanos y funcionarios públicos en seguridad de la información.

Lo anterior tiene una razón de ser, crear una cultura de seguridad de la información, que se constituya en el primer anillo de seguridad para minimizar el riesgo de un ciberataque o, peor aún, una ciberguerra, con funcionarios y ciudadanos bien educados en el campo de la seguridad de la información. Buenas prácticas y buenos hábitos constituirán un blindaje inicial para proteger el activo más valioso de toda organización, la información en todas sus modalidades.

4. Conclusiones

- La mayoría de analistas y especialistas militares concluyen que la vida del presente mundo incluirá ciberataques y estamos *ad portas* de una ciberguerra.

- Se estima que cada año la pérdida total por delitos informáticos es mucho mayor de lo que se cree. En realidad, nadie sabe con seguridad la dimensión del delito, ya que una buena parte no se detecta o no denuncia.

Foto: Student Technological Applications and Services Ltd. Getting-in.

- La seguridad nunca es absoluta y, por lo tanto, siempre es mejorable.
- La lucha contra la ciberguerra se da con un trabajo en equipo y una excelente cultura informática.
- El analista de sistemas estudia lo que puede suceder, pero los que valoran los daños y deciden las medidas que se han de adoptar son los directivos, con la asesoría del área de seguridad de la información.
- El análisis de seguridad de riesgos en la información debe comenzar con el análisis del sistema.
- No se debe invertir en seguridad una cantidad mayor que lo que suponga la exposición al riesgo que se debe proteger.
- Se debe prestar especial atención a los sucesos que aparentemente no tienen importancia, pero que por su frecuencia suponen un elevado riesgo.
- Educar, entrenar y coordinar son las claves del éxito, junto con un ambicioso programa de concientización en seguridad de la información.
- Los ciberataques y, por ende, la ciberguerra, no tienen fronteras.
- No se ve en la actualidad un mundo libre de ciberataques.
- Con base en la anterior conclusión, minimiza la eficacia de un sistema de disuasión cibernética, cuya razón de ser es la prevención de estos ataques.
- Un factor fundamental en la seguridad de la información como llave del éxito contra la ciberguerra es el recurso humano, que debe tener una clara conciencia de la amenaza real del presente siglo. Con una buena educación en ciberseguridad y entrenamiento apropiado, se puede minimizar el riesgo de los ciberataques y de una ciberguerra.
- Siempre se debe analizar y considerar el triángulo de la seguridad de la información: la confiabilidad, la oportunidad y la disponibilidad, para brindarle las medidas preventivas y minimizar el riesgo de un incidente de seguridad.

5. Bibliografía

- Air&Space, Power, Journal, volumen 24, tercer trimester 2012.
- Adaptación de la Fuerza Conjunta Cibernética a la Guerra Asimétrica, Documentos de Seguridad y Defensa, Centro De Estudios De la Defensa Nacional, Numero 44, octubre 2011.
- Apuntes Curso XLI, de Estrategia y Política de Defensa (SDP), marzo 2013, CHDS.
- Documento Conpes 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa, 14 de julio de 2012.
- Cuadernos de Estrategia, número 149, Ciberseguridad, Retos y Amenazas a la seguridad Nacional en el Ciberespacio. Instituto Español de Estudios Estratégicos.

La seguridad de la información es el primer eslabón de la cadena que permite reducir o minimizar el riesgo, pues no existe la garantía total de inmunidad a un ataque cibernético.

CURRÍCULUM

Coronel (RA) Jairo Andrés Cáceres García; Docente-investigador de la Cátedra de Ciberguerra en la ESDEGUE. Oficial en uso de buen retiro del Ejército Nacional. Autor del Manual de Seguridad informática para el Ejército. Gerente militar creador del programa Sistema de Información Logística -SILOG- del Sector Defensa. Maestro en Ingeniería de Sistemas Logísiticos de la Pontificia Universidad Católica de Valparaiso y Academia Politécnica Militar del Ejército de Chile. Especialista en Informática y Telecomunicaciones de la Universidad Autónoma de Guadalajara México. Consultor en seguridad de la información de empresas privadas.